

VIRGINIA ECONOMIC DEVELOPMENT PARTNERSHIP

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2024

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Economic Development Partnership (Partnership) as of and for the year ended June 30, 2024, and issued our report thereon, dated June 1, 2025. Our report, included in the Partnership's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the Partnership's website at www.vedp.org. Our audit of the Partnership found:

- the financial statements are presented fairly, in all material respects; and

- three matters involving internal control and its operation requiring management's attention, that also represent instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards; however, we do not consider the matters to be material weaknesses.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Section 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

–TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Information Security Program and IT Governance
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

The Virginia Economic Development Partnership (Partnership) continues to make improvements to their information security program and IT governance structure to address the issues identified during our fiscal year 2022 audit. However, the Partnership has not yet finished implementing corrective actions and most remain outstanding. We communicated four control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls

The Partnership's adopted security standard, the Commonwealth's Information Security Standard, SEC530 (Security Standard) requires the agency head to maintain an information security program that is sufficient to protect the agency's IT systems and to ensure the information security program is documented and effectively communicated. Not having a comprehensive and updated IT governance structure to properly manage the Partnership's IT environment and information security program can result in a data breach or unauthorized access to confidential and mission critical data, leading to data corruption, data loss, or system disruption if accessed by a malicious attacker, either internal or external.

The Partnership has not yet completed remediation efforts to improve its information security program and IT governance structure due to the time required to complete all remediation efforts, changes to the remediation plan, and resource constraints. The Partnership should bring its IT security program in compliance with the Security Standard. Specifically, the Partnership should implement IT governance changes to address the control deficiencies discussed in the communication marked FOIAE. Implementing these recommendations will help to ensure the Partnership protects the confidentiality, integrity, and availability of its sensitive and mission critical data.

Improve Service Provider Oversight
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

The Partnership has made progress since our last audit but should finish implementing and documenting the necessary processes to manage risks from the use of external information system services, including monitoring the effectiveness of security controls of external service providers (providers). Providers are organizations that perform certain business tasks or functions on behalf of the Partnership and the Commonwealth. The Partnership uses 27 providers for business functions that include the processing and storing of sensitive data.

The Security Standard states that management remains accountable for maintaining compliance with the Security Standard through documented agreements with providers and oversight of services provided. Additionally, the Security Standard requires that organizations document system and services acquisition policies and procedures. The Security Standard also details requirements for organizations to follow to manage external service providers. By not defining, documenting, and employing a process to gain continuous assurance over providers' operating controls, the Partnership cannot validate the providers have effective security controls to protect the Partnership's sensitive and confidential data.

Resource constraints and other priorities have limited the Partnership's progress on this issue. The Partnership has not yet completed a procedure to facilitate the implementation of the existing policy and associated controls, and has not yet communicated required security controls, roles, and responsibilities via documented agreements with its providers. The Partnership obtained an independent audit assurance report over each of its 27 hosted systems, created a Report Evaluation Form to document its evaluation of reports, and used the form to review and evaluate the independent audit assurance report for two providers. However, the Partnership has not completed a formal review and evaluation of each of the remaining reports due to resource constraints.

The Partnership should complete, approve, and implement procedures to monitor the effectiveness of security controls of external service providers. The Partnership should then communicate the required security controls, as well as the roles and responsibilities of each party, through documented agreements with its providers. Additionally, the Partnership should continue to obtain annual independent audit assurance reports from each provider and evaluate the independent audit assurance reports received to ensure the provider has effective operating controls to protect the Partnership's sensitive and mission critical data. During the evaluation, the Partnership should identify control deficiencies, develop mitigation plans, escalate issues of non-compliance, and implement complementary user entity controls, as needed. Finally, the Partnership should document its evaluation of each of the independent audit assurance reports using its new Report Evaluation Form. Gaining sufficient assurance over each provider's security controls will help to ensure the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve Virtual Private Network Security

Type: Internal Control and Compliance
Severity: Significant Deficiency

The Partnership does not manage its Virtual Private Network (VPN) in accordance with the Security Standard. The Security Standard requires the implementation of certain security controls to safeguard critical systems that contain or process sensitive data.

We identified and communicated two specific control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls. The Partnership should dedicate the necessary resources to remediate the control weaknesses communicated in the FOIAE recommendation to ensure the Partnership secures it network to protect its systems and data.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

June 1, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Directors
Virginia Economic Development Partnership

Jason El Koubi, President and CEO
Virginia Economic Development Partnership

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the governmental activities and each major fund of the **Virginia Economic Development Partnership** (Partnership) as of and for the year ended June 30, 2024, and the related notes to the financial statements, which collectively comprise the Partnership's basic financial statements, and have issued our report thereon dated June 1, 2025.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the Partnership's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Partnership's internal control. Accordingly, we do not express an opinion on the effectiveness of the Partnership's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Improve Information Security Program and IT Governance," "Improve Service Provider Oversight," and "Improve Virtual Private Network Security" which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Partnership's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards, and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings and recommendations titled **"**Improve Information Security Program and IT Governance," "Improve Service Provider Oversight," and "Improve Virtual Private Network Security."

The Partnership's Response to Findings

We discussed this report with management at an exit conference held on May 29, 2025. Government Auditing Standards require the auditor to perform limited procedures on the Partnership's response to the findings identified in our audit, which is included in the accompanying section titled "Partnership Response." The Partnership's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

The Partnership has not completed adequate corrective action with respect to the prior reported findings identified as ongoing in the Findings Summary included in the Appendix.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

LCW/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Issued
Improve Information Security Program and IT Governance	Ongoing	2022
Improve Service Provider Oversight	Ongoing	2022
Improve Virtual Private Network Security	Ongoing	2024

*A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

June 9, 2025

Ms. Staci A. Henshaw
Auditor of Public Accounts
James Monroe Building
101 N. 14th Street
Richmond, Virginia 23219

Dear Ms. Henshaw:

The Virginia Economic Development Partnership (VEDP) has reviewed the findings and recommendations provided by the Auditor of Public Accounts (APA) as part of your audit of VEDP's financial records for the year ended June 30, 2024. VEDP appreciates the opportunity to respond to the Internal Control and Compliance Findings and Recommendations included in your report, and we give your comments the highest level of consideration.

Internal Control and Compliance Findings and Recommendations

Improve Information Security Program and IT Governance

VEDP continues to strengthen its information security program and IT governance structure. Over the past year, we have made significant progress in addressing this finding. VEDP expanded its risk management and contingency planning efforts across all departments, completed formal data classification and risk assessments, and is now working to integrate these results into our continuity and disaster recovery plans.

VEDP has completed the sensitive system audits for the systems identified in the VEDP IT Audit Plan. VEDP is actively testing the new financial system with plans to move into the system and operate from it exclusively starting at the beginning of FY2026. While some of these improvements were not within the scope of the APA's audit testing for FY2024, we anticipate substantial completion of all remediation efforts by January 2026, in time for the APA's FY2025 audit.

Improve Service Provider Oversight

VEDP has made significant efforts to improve service provider oversight and is working diligently to ensure all service providers have been properly evaluated using our Vendor Risk Assessment. VEDP has obtained and analyzed SOC reports, secured Trust Center access, and assessed and scored our providers to ensure continued oversight. VEDP will continue reviewing all provider reports, documenting our evaluations, and mitigating any identified gaps. VEDP hopes to review the service provider oversight improvements with the APA during the course of the FY2025 audit.

Improve VPN Security

VEDP acknowledges the finding to improve VPN security through alignment with the Commonwealth security standard. VEDP is confident in the security of the VPN and has made the configuration and documentation changes to best align with the standard. VEDP is actively testing these changes for mission impact and plans to show compliance or documented exceptions during the course of the FY2025 audit.

901 E. Cary Street, Suite 900
Richmond, Virginia 23219
VEDP.org

We are very appreciative of the courtesy and professionalism with which the APA team conducted this year's audit. We also appreciate their patience as we gathered the requested documentation in the course of the audit.

Sincerely,

Jason El Koubi
President and CEO

901 E. Cary Street, Suite 900
Richmond, Virginia 23219
VEDP.org